In the Claims:

1. (Currently Amended) A method for secure distribution of digital content to an untrusted environment of an intended recipient of said digital content, comprising the steps of: constructing a trusted environment within said untrusted environment;

constructing <u>from said digital media</u> at least two digital inputs <u>sources</u>, said <u>digital</u> inputs <u>sources</u> being operable in combination in order to produce a <u>screen</u> rendered version of said digital content;

transferring to said trusted environment such that each of said inputs sources_is transmitted via a different path, and;

combining said inputs <u>sources</u> within said trusted environment in order to produce said <u>screen</u> rendered version of digital content, said trusted environment otherwise preventing access to said digital inputs <u>sources</u>.

- 2. (Original) A method according to claim 1 wherein said digital content is a document.
- 3. (Previously Presented) A method according to claim 1 wherein said digital content is multimedia digital content.
- 4 5. (Canceled).
- 6. (Original) A method according to claim 3 wherein said multimedia digital content consists of at least two different streams.
- 7 10. (Canceled).
- 11. (Currently Amended) A method according to claim 1 wherein said trusted environment comprises a software component.
- 12 14. (Canceled).

- 15. (Previously Presented) A method according to claim 1 wherein said trusted environment comprise a hardware component.
- 16. (Canceled).
- 17. (Currently Amended) A method according to claim 1 wherein said trusted environment comprises a firmware component.
- 18 20. (Canceled).
- 21. (Currently Amended) A method according to claim 1 wherein said trusted environment comprises at least two components.
- 22. (Original) A method according to claim 21 wherein at least one of said components comprises a software component.
- 23 34. (Canceled).
- 35. (Currently Amended) A method according to claim 1 wherein at least one of said inputs comprises of a scrambled copy of said digital content, and at least one other input comprises the information needed for said reproduction.
- 36. (Currently Amended) A method according to claim 1 wherein a group of at least two of said inputs comprises of a function of a scrambled copy of said digital content, and at least one other input comprises of the information needed for reconstruction.
- 37 58. (Canceled).
- 59. (Previously Presented) A method according to claim 1 wherein said digital content is split into said separate inputs in a trusted server, said server is operable to deliver said digital content to said relatively trusted environment in the form of said separate inputs.

60 - 61. (Canceled).

62. (Currently Amended) A method according to claim 1, for secure distribution of digital content further comprising the steps of:

gathering input from at least one source;

producing trustworthiness credentials about said digital content's intended recipient environment based on said input;

evaluate said intended recipient environment's trustworthiness credentials; determine a distribution policy according to said trustworthiness credentials evaluation, and;

performing decisions about said distribution according to said policy.

- 63 70. (Canceled).
- 71. (Original) A method according to claim 62 wherein said credentials comprise information gathered in the past.
- 72 73. (Canceled).
- 74. (Original) A method according to claim 62 wherein said credentials comprise of information about the environment into which said digital content is to be distributed.
- 75 79. (Canceled).
- 80. (Previously Presented) A method according to claim 62 wherein said credentials comprise of reports from at least one trusted component.
- 81 107. (Canceled).

108. (Currently Amended) A method for secure distribution of digital content comprising the steps of:

transferring said digital content to an untrusted environment;

using a relatively trusted environment within said untrusted environment, said trusted environment being operable to produce a rendered version of said digital content and further being comprised of mechanisms to restrict tampering thereof, wherein said version is rendered for a display.

- 109. (Previously Presented) A method according to claim 108 wherein said trusted environment comprise at least two components.
- 110 115. (Canceled).
- 116. (Previously Presented) A method according to claim 109 wherein said components comprise a watchdog component wherein said watchdog component is capable of monitoring other components of the trusted environment.
- 117. (Original) A method according to claim 116 wherein said monitoring comprise of authentication.
- 118 -119. (Canceled).
- 120. (Original) A method according to claim 117 wherein said authentication comprise authentication of the code of the component.
- 121 123. (Canceled).
- 124. (Original) A method according to claim 116 wherein said monitoring comprises monitoring of the operation of said components.
- 125. (Original) A method according to claim 124 wherein said monitoring of the operation of said components comprises monitoring of used interfaces.

126 - 151. (Canceled).

152. (Previously Presented) A method according to claim 109 wherein at least one of said components comprise a plurality of interfaces and functionality to monitor at least one of said interfaces.

153 - 156. (Canceled).

157. (Previously Presented) A method according to claim 152, wherein said method comprises functionality to monitor at least one of said interfaces used by the underlying system.

158 - 165. (Canceled).

166. (Previously Presented) A method according to claim 108 wherein said trusted environment comprise mechanism to restrict copying of at least one of the outputs said trusted environment generates.

167 - 173. (Canceled).

174. (Previously Presented) A method according to claim 166 wherein said mechanism to restrict copying is comprised of altering the output in order to change a quality of the copy which is produced by said copying.

175 - 179. (Canceled).